CLAIMS

1. A method of arranging communication between an administrator device (AC) and an administered device (AE, AS) in a network, the method including the steps of:

- arranging said communication in the form of a chain of digitally signed communication items including messages sent from an originator device (AC resp. AS, AE) to a recipient device (AS, AE resp. AC), each said message having associated a respective digitally signed receipt, and

- configuring said originator device (AC resp. AS, AE) not to send a new item towards said recipient device (AS, AE resp. AC) in the absence of a respective digitally signed receipt for a previously sent item.

2. The method of claim 1, characterized in that it includes the steps of:

- detecting at said originator device (AC resp. AS, AE) a respective digitally signed receipt item from said recipient device (AS, AE resp. AC) having failed to reach the originator device (AC resp. AS, AE) within a given time span after a message item has been issued by said originator device (AC resp. AS, AE), and

- asking said recipient device (AS, AE resp. AC) for a signed statement indicating at least one of the last message item received and the last message item sent by said recipient device (AS, AE resp. AC).

3. The method of claim 1, characterized in that it includes the step of storing with at least one of said administrator device (AC) and said administered device (AS, AE) a history record of communication items exchanged therebetween, said history record being

agreed upon and signed by both said administrator device (AC) and said administered device (AS, AE).

4. The method of claim 1, characterized in that it includes the step of carrying out at said originator device (AC resp. AS, AE) a session closing step mentioning at least one of the last message item received and the last message item sent by said recipient device (AS, AE resp. AC).

5. The method of claim 1, characterized in that it includes the step of keeping with said originator device (AC resp. AS, AE) an indication of an on-going communication session as a pending session until a signed receipt item is received from said recipient device (AS, AE resp. AC).

6. The method of claim 1, characterized in that it includes the step of inserting in said communication items payload data and administrative commands accompanied by respective digital signatures.

7. The method of claim 1, characterized in that it includes the step of causing said recipient device (AS, AE resp. AC) to verify said digital signatures for validity.

8. The method of claim 1, characterized in that it includes the step of creating said digital signatures under the full and univocal control of the device (AC resp. AS, AE) issuing such signatures.

9. The method of claim 1, characterized in that it includes the step of associating secure digital signature evidence with said digitally signed messages and receipts.

10. The method of claim 9, characterized in that said secure digital signature evidence is in the form of RSA class digital signatures.

11. The method of claim 1, characterized in that it includes the step of arranging communication between a

set of administrator devices (AC) and a given administered device (AS, AE), the method including the step of permitting at least one administrator device (AC) in said set to hide its identity to said administered device (AS, AE).

12. The method of claim 11, characterized in that it includes the step of said at least one administrator device (AC) hiding its identity to said administered device (AS, AE) by using at least one of group signatures or pseudonym digital certificates.

13. The method of claim 11, characterized in that it includes the step of resuming a session interrupted in the absence of a receipt provided by said at least one administrator (AC) hiding its identity to a message sent by said given administered device (AS, AE), wherein said session is resumed by said at least one administrator (AC) hiding its identity.

14. A system of an administrator device (AC) and an administered device (AE, AS) in a network, said administrator device (AC) and administered device (AE, AS) being configured for communication in the form of a chain of digitally signed communication items including messages sent from an originator device (AC resp. AS, AE) to a recipient device (AS, AE resp. AC), each said message having associated a respective digitally signed receipt, and wherein said originator device (AC resp. AS, AE) is configured not to send a new item towards said recipient device (AS, AE resp. AC) in the absence of a respective digitally signed receipt for a previously sent item.

15. The system of claim 14, characterized in that:

- said originator device (AC resp. AS, AE) is configured for detecting a respective digitally signed receipt item from said recipient device (AS, AE resp. AC) having failed to reach the originator device (AC

resp. AS, AE) within a given time span after a message item has been issued by said originator device (AC resp. AS, AE), and

- asking said recipient device (AS, AE resp. AC) for a signed statement indicating at least one of the last message item received and the last message item sent by said recipient device (AS, AE resp. AC).

16. The system of claim 14, characterized in that it includes, stored with at least one of said administrator device (AC) and said administered device (AS, AE), data items comprising a history record of communication items exchanged therebetween, said history record being agreed upon and signed by both said administrator device (AC) and said administered device (AS, AE).

17. The system of claim 14, characterized in that said originator device (AC resp. AS, AE) is configured for carrying out a session closing step mentioning at least one of the last message item received and the last message item sent by said recipient device (AS, AE resp. AC).

18. The system of claim 14, characterized in that said originator device (AC resp. AS, AE) is configured for keeping an indication of an on-going communication session as a pending session until a signed receipt item is received from said recipient device (AS, AE resp. AC).

19. The system of claim 14, characterized in that said originator device (AC resp. AS, AE) is configured for inserting in said communication items payload data and administrative commands accompanied by respective digital signatures.

20. The system of claim 14, characterized in that said recipient device (AS, AE resp. AC) is configured for verifying said digital signatures for validity.

21. The system of claim 14, characterized in that it includes means for creating said digital signatures said means being assigned univocally and acting under the full control of the device (AC resp. AS, AE) issuing such signatures.

22. The system of claim 14, characterized in that it is configured for associating secure digital signature evidence with said digitally signed messages and receipts.

23. The system of claim 22, characterized in that said secure digital signature evidence is in the form of RSA class digital signatures.

24. The system of claim 14, characterized in that it includes a set of administrator devices (AC) and a given administered device (AS, AE), wherein at least one administrator device (AC) in said set is configured to hide its identity to said administered device (AS, AE).

25. The system of claim 24, characterized in that said at least one administrator device (AC) is configured for hiding its identity to said administered device (AS, AE) by using at least one of group signatures or pseudonym digital certificates.

26. The system of claim 24, characterized in that said at least one administrator (AC) hiding its identity is configured for resuming a session interrupted in the absence of a receipt provided by said at least one administrator (AC) hiding its identity to a message sent by said given administered device (AS, AE).

27. A communication network including a system according to any of claims 14 to 26.

28. Computer program product, loadable in the memory of at least one computer and including software

code portions for performing the steps of the method of any of claims 1 to 13.